IMPLEMENTASI HYBRID METODE CNN-FACIAL LANDMARK DETECTION-LIVENESS DETECTION DALAM SISTEM ABSENSI PENGENALAN WAJAH

PROPOSAL SKRIPSI

Diajukan sebagai Salah Satu Syarat untuk Mendapatkan
Gelar Sarjana Komputer (S.Kom) Program Studi Informatika

ANDI MUHAMMAD AKBAR DB
105841111221

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH MAKASSAR

2025

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Segala puji bagi Allah Subhanahu Wata'ala, atas limpahan rahmat dan Karunia-Nya sehingga penulis dapat menyelesaikan penyusunan Proposal Skripsi ini yang berjudul "**IMPLEMENTASI HYBRID METODE CNN-FACIAL LANDMARK DETECTION-LIVENESS DETECTION DALAM SISTEM ABSENSI PENGENALAN WAJAH**". Shalawat beserta salam senantiasa penulis panjatkan kepada Nabi besar Muhammad SAW sebagai uswatun hasanah dan rahmatan lil alamin.

Dalam penyusunan Proposal Skripsi ini penulis mengucapkan banyak terima kasih kepada semua pihak yang telah membantu dan memberikan motivasi serta bimbingan dan arahan dalam penyusunan Proposal Skripsi ini,terutama kepada:

1. Kedua orang tua yang selalu memberikan dukungan baik berupa moral, materi, dan spiritual agar dapat terselesaikannya penyusunan Proposal Skripsi ini.
2. Ibu **Dr.Ir.Hj Nurnawati, S.T., M.T., I.P.M,** selaku Dekan Fakultas Teknik Universitas Muhammadiyah Makassar.
3. Bapak **Muh. Syafa'at S Kuba, S.T., M.T,** selaku Wakil Dekan Fakultas Teknik Universitas Muhammadiyah Makassar.
4. Bapak **Muhyiddin A. M. Hayat. S.Kom., M.T,** selaku Ketua Program Studi Informatika Fakultas Teknik Universitas Muhammadiyah Makassar sekaligus selaku Dosen Pembimbing 2 yang telah memberikan arahan dan bimbingan serta saran yang sangat berarti dalam penyusunan proposal ini.
5. Bapak **Ir. Muhammad Faisal, S.SI., M.T., Ph.D., IPM** selaku Dosen Pembimbing 1 sekaligus sebagai Dosen Pembimbing Akademik yang telah memberikan arahan dan bimbingan serta saran yang sangat berarti dalam penyusunan proposal ini.

6. Seluruh Dosen Fakultas Teknik Program Studi Informatika Universitas Muhammadiyah Makassar yang telah memberikan ilmu dan bantuannya dalam penulisan proposal ini.
7. Teman-teman angkatan 2021 Program Studi Informatika Fakultas Teknik Universitas Muhammadiyah Makassar dan teman teman diluar dari kampus, khususnya Teman-teman Kelas D Informatika, terima kasih atas dukungan dan doanya.
8. Kepada semua pihak yang tidak bisa penulis sebutkan satu persatu, penulis mengucapkan banyak terima kasih yang sebesar-besarnya.

Demikian Proposal Skripsi ini dan penulis menyadari bahwa proposal ini masih memiliki banyak kekurangan didalamnya oleh karena itu kritik dan saran yang sifatnya membangun dari pembaca sangat kami harapkan.

Billahi fii sabililhaq, fastabiqul khairat.

Wassalamualaikum Wr. Wb.

Makassar ,27 Mei 2025

Penulis

Andi Muhammad Akbar DB

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

A. Latar Belakang

Sistem absensi pada berbagai institusi, baik pendidikan maupun perkantoran, telah lama diketahui memakan waktu dan rentan terhadap kesalahan manusia. Seiring dengan kemajuan teknologi, kebutuhan akan sistem absensi otomatis yang lebih efisien, akurat, dan aman semakin meningkat. Teknologi pengenalan wajah muncul sebagai salah satu solusi yang menjanjikan, menawarkan metode absensi yang bersifat *contactless* (tanpa sentuh), cepat, dan intuitif bagi pengguna (Devrani et al., 2024). Pengenalan wajah telah banyak diaplikasikan dalam berbagai bidang, termasuk untuk sistem kehadiran (Nemavhola et al., 2025), dan popularitasnya meningkat karena proses otentikasi *contactless* yang relatif berbiaya rendah (Raj et al., 2021).

Meskipun memiliki banyak keunggulan, sistem pengenalan wajah tidak luput dari ancaman keamanan, salah satunya adalah serangan *spoofing* atau pemalsuan. Ancaman ini terjadi ketika pihak yang tidak bertanggung jawab mencoba mengelabui sistem dengan menggunakan foto cetak, rekaman video, topeng 3D, atau artefak lainnya (Raj et al., 2021). Sistem pengenalan wajah secara inheren rentan terhadap serangan spoofing semacam ini dan memerlukan mekanisme deteksi keaktifan (*liveness detection*) untuk memastikan bahwa wajah yang dipindai adalah wajah manusia asli yang hadir secara fisik. Banyak sistem absensi berbasis wajah yang ada saat ini masih rentan terhadap serangan spoofing, yang secara signifikan mengurangi tingkat keamanan dan keandalannya (Chautharia et al., 2024).

Dalam penelitian ini digunakan pendekatan *hybrid* yang tidak sekadar menggabungkan metode, melainkan membangun arsitektur *pipeline* yang terpisah. *Convolutional Neural Network* (CNN) digunakan secara khusus untuk pengenalan identitas dengan mengekstraksi *feature vector* unik dari setiap

wajah. CNN sendiri pertama kali diperkenalkan oleh LeCun dkk. dan sejak itu terbukti unggul dalam tugas pengenalan pola dan visi komputer, termasuk pengenalan wajah (Nemavhola et al., 2025). Sementara itu, deteksi keaktifan dilakukan melalui analisis *facial landmark* yang dapat memantau isyarat alami seperti kedipan mata atau gerakan mulut (Zhi Jie et al., 2023).

Pemisahan tugas ini memberikan keuntungan dari sisi efisiensi. Sistem akan lebih dahulu menjalankan *liveness Detection* yang ringan. Jika wajah gagal diverifikasi, proses langsung dihentikan sehingga CNN yang membutuhkan komputasi lebih besar tidak perlu dijalankan. Namun, desain ini juga menimbulkan *trade-off* kegagalan modul landmark akibat pencahayaan buruk atau pose ekstrem dapat membuat autentikasi gagal meskipun CNN sebenarnya mampu mengenali wajah.

Perkembangan teknologi *spoofing* yang semakin canggih, seperti kemunculan deepfakes dan teknik injeksi video berkualitas tinggi , mendorong evolusi berkelanjutan dalam teknik deteksi keaktifan. Metode deteksi keaktifan bergerak dari analisis statis sederhana menuju analisis dinamis yang lebih kompleks dan pendekatan multi-modal.

Adopsi teknologi pengenalan wajah yang semakin meluas, didorong oleh pertumbuhan pasar global yang signifikan, secara tidak langsung juga meningkatkan insentif bagi para pelaku kejahatan untuk mengembangkan teknik spoofing yang lebih canggih. Fenomena ini, pada gilirannya, memicu penelitian dan pengembangan yang lebih intensif di bidang deteksi keaktifan sebagai mekanisme pertahanan krusial. Kegagalan dalam mengimplementasikan deteksi keaktifan yang robust tidak hanya akan mengakibatkan pencatatan absensi yang tidak akurat, tetapi juga berpotensi membuka celah keamanan yang lebih luas, terutama jika sistem absensi terintegrasi dengan data atau sistem sensitif lainnya (Gupta, 2024).

Berdasarkan permasalahan yang ditemukan, diperlukan pendekatan hybrid yang mengintegrasikan beberapa teknologi canggih, seperti *(CNN)* untuk

pengenalan identitas yang akurat, deteksi landmark wajah untuk analisis fitur yang presisi, dan modul deteksi keaktifan yang tangguh. Kombinasi ini diharapkan dapat menciptakan sistem absensi pengenalan wajah yang tidak hanya akurat dalam mengenali individu, tetapi juga kuat dalam menghadapi berbagai jenis serangan spoofing dan mampu beradaptasi dengan variasi kondisi dunia nyata, seperti perubahan pencahayaan dan pose wajah (Chautharia et al., 2024).

B. Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana mengaplikasikan metode CNN pada sistem absensi pengenalan wajah?
2. Bagaimana mengembangkan mekanisme deteksi keaktifan berbasis analisis gerakan dinamis landmark wajah untuk membedakan wajah asli dan upaya pemalsuan seperti foto atau video?
3. Strategi anti-spoofing apa yang paling efektif untuk menghadapi serangan video seperti replay attack dan deepfake dalam sistem absensi?

C. Tujuan Penelitian

1. Mengaplikasikan metode CNN pada sistem absensi pengenalan wajah.
2. Mengevaluasi kinerja sistem secara komprehensif, meliputi akurasi pengenalan identitas, efektivitas deteksi keaktifan terhadap berbagai jenis serangan spoofing (terutama serangan foto dan video replay), toleransi sistem terhadap variasi kemiringan wajah, dan kecepatan pemrosesan keseluruhan.
3. Mengimplementasikan modul deteksi landmark wajah yang akurat dan mampu beroperasi secara real-time, misalnya dengan memanfaatkan pustaka seperti MediaPipe yang mampu mendeteksi hingga 468 landmark wajah 3D , sebagai dasar untuk proses pengenalan dan deteksi keaktifan.

D. Manfaat Penelitian

1. Terhadap Penulis

   Kontribusi penelitian ini bagi penulis adalah memberikan pemahaman yang lebih mendalam mengenai integrasi metode CNN, deteksi landmark wajah, dan berbagai teknik deteksi keaktifan (khususnya yang berbasis analisis gerakan landmark) untuk pengembangan sistem biometrik yang lebih aman dan andal.

2. Terhadap Pembaca

   Kontribusi penelitian ini bagi pembaca adalah menghasilkan sebuah prototipe sistem absensi otomatis yang lebih aman, akurat, dan efisien, yang memiliki potensi untuk diterapkan secara luas di berbagai institusi pendidikan maupun perusahaan.

E. Ruang Lingkup Penelitian

Dalam rangka menjaga fokus dan kelayakan penelitian dalam batasan waktu dan sumber daya yang tersedia, beberapa batasan ditetapkan sebagai berikut:

1. Jenis serangan spoofing yang akan menjadi target pengujian primer adalah serangan menggunakan foto cetak, foto digital yang ditampilkan pada layar perangkat lain (misalnya, smartphone atau tablet), dan serangan video replay. Serangan yang menggunakan topeng 3D fisik berkualitas tinggi atau teknik deepfake yang sangat canggih, yang mungkin memerlukan sensor kedalaman khusus atau metode analisis yang jauh lebih kompleks, tidak akan menjadi fokus utama pengujian , meskipun kesadaran akan ancaman ini tetap ada.
2. Toleransi sistem terhadap kemiringan wajah akan diuji hingga batas tertentu (misalnya, ±45 derajat atau sesuai dengan kemampuan model yang berhasil dikembangkan). Meskipun target ideal seperti ±90 derajat akan menjadi acuan, pencapaian batas tersebut mungkin memerlukan teknik yang lebih kompleks yang berada di luar batasan saat ini.
3. Studi ini difokuskan pada pendekatan yang diusulkan tanpa bertujuan melakukan komparasi dengan metode atau aplikasi yang telah ada.

F. Sistematika Penulisan

Secara garis besar penulisan laporan tugas akhir ini terbagi menjadi beberapa bab yang tersusun sebagai berikut:

BAB I PENDAHULUAN

Bab ini menerangkan secara singkat dan jelas mengenai latar belakang penulisan penelitian tugas akhir, rumusan masalah, tujuan dan manfaat, batasan permasalahan, metodologi yang digunakan dan sistematika penulisan.

BAB II TINJAUUAN PUSTAKA

Pada bab ini membahas tentang teori-teori yang melandasi penulis dalam melaksanakan penelitian.

BAB III METODE PENELITIAN

Membahas tentang metode penelitian dan alat yang digunakan untuk pembuatan sistem.

BAB II
TINJAUAN PUSTAKA

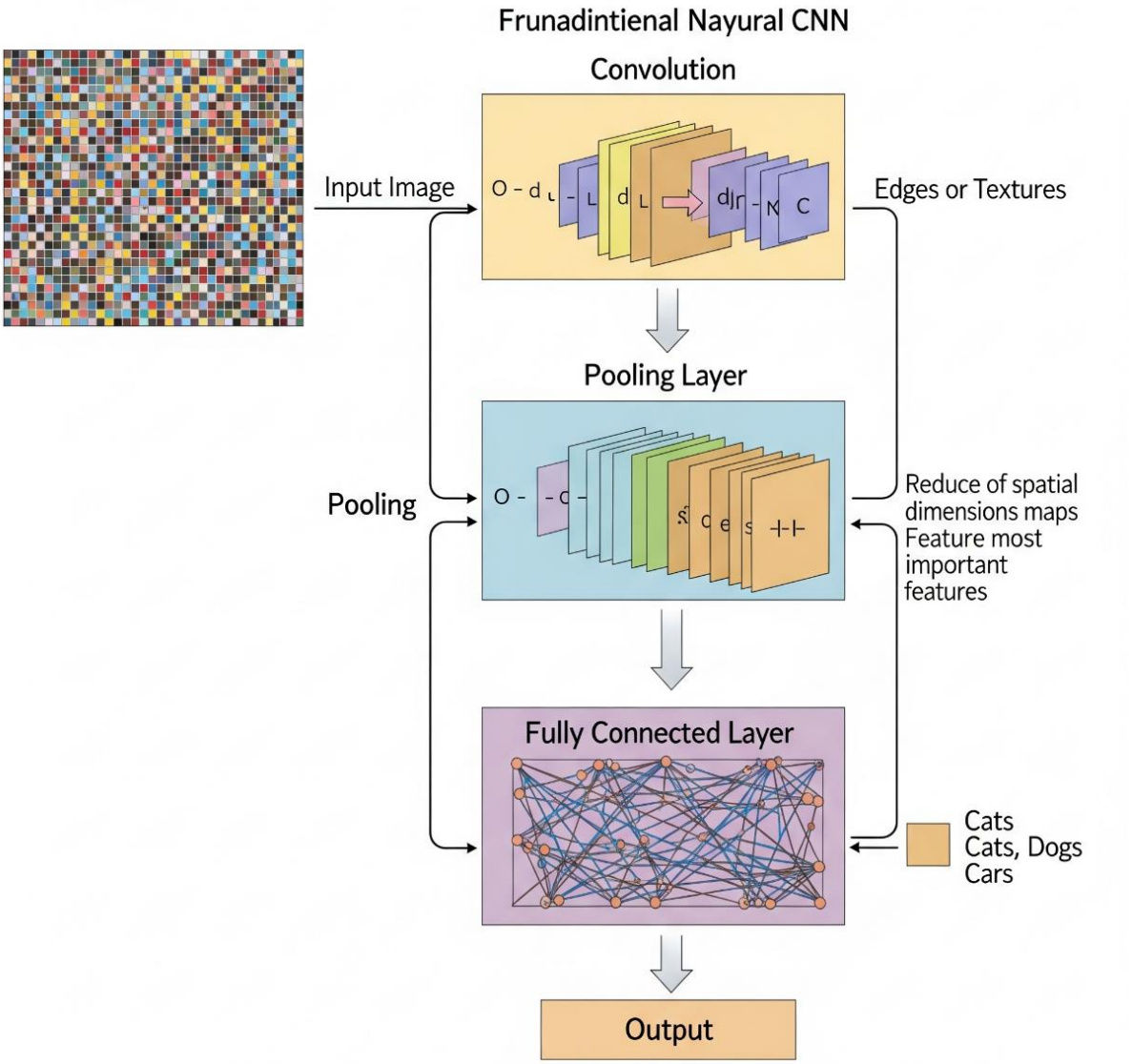
A. Landasan Teori

1. Convolutional Neural Network (CNN)

Convolutional Neural Network (CNN) merupakan salah satu jenis arsitektur deep learning yang sangat efektif dalam tugas-tugas visi komputer, termasuk pengenalan wajah. CNN terdiri dari beberapa lapisan utama, yaitu lapisan konvolusi (*convolutional layer*) yang bertugas mengekstraksi fitur dari gambar input, lapisan pooling yang mengurangi dimensi spasial fitur, lapisan *fully connected* yang melakukan klasifikasi berdasarkan fitur yang telah diekstraksi, dan fungsi yang memperkenalkan non-linearitas ke dalam model (S et al., 2023).

Dalam sistem pengenalan wajah, CNN memainkan peran krusial dalam beberapa tahapan, mulai dari deteksi wajah awal dalam sebuah gambar atau video, pra-pemrosesan gambar wajah, ekstraksi fitur-fitur diskriminatif dari wajah, hingga klasifikasi atau pencocokan wajah untuk menentukan identitas (Nemavhola et al., 2025). Tahap ekstraksi fitur dianggap sebagai salah satu aspek paling fundamental dan menantang dalam pengenalan wajah (Pavan dan Thanuja, 2023), di mana CNN unggul karena kemampuannya untuk secara otomatis mempelajari dan mengekstrak hierarki fitur yang relevan langsung dari data gambar mentah (Nemavhola et al., 2025).

Kemampuan CNN dalam mengotomatisasi proses ekstraksi fitur ini menjadikannya fondasi penting dalam pengembangan sistem absensi berbasis pengenalan wajah. Dengan akurasi tinggi dan kecepatan pemrosesan yang efisien, CNN memungkinkan sistem absensi mendeteksi dan mengenali wajah pengguna secara real-time, yang sangat mendukung penerapan teknologi ini dalam lingkungan pendidikan maupun industri. Literasi lapisan dasar pada CNN ditampilkan pada gambar 1.



Gambar 1. Ilustrasi Lapisan Dasar Convolutional Neural Network (CNN)

a. Arsitektur CNN

Sejumlah arsitektur CNN telah dikembangkan dan terbukti efektif untuk tugas pengenalan wajah. Pemilihan arsitektur yang tepat seringkali melibatkan pertimbangan antara akurasi, kecepatan komputasi, dan ukuran model. Beberapa arsitektur yang menonjol meliputi:

1) *VGGNet* (misalnya, VGG16, *VGGFace*): Dikenal karena strukturnya yang dalam dan penggunaan filter konvolusi berukuran kecil (3x3 secara konsisten). Arsitektur ini telah

menunjukkan akurasi yang sangat tinggi, seringkali di atas 98%, pada dataset *benchmark* seperti Label *Faces in the Wild* (LFW) dan *VGGFace*. Sebagai contoh, VGG16 dilaporkan mencapai akurasi 98.95% pada dataset *VGGFace* (Nemavhola et al., 2025).

2) *FaceNet:* Dikembangkan oleh Google, *FaceNet* menggunakan pendekatan pembelajaran embedding wajah secara langsung dengan memanfaatkan *triplet loss function*. Metode ini memungkinkan model untuk memetakan wajah ke dalam ruang fitur di mana jarak antar *embedding* merepresentasikan kemiripan wajah. *FaceNet* menunjukkan kinerja yang sangat kuat, misalnya mencapai akurasi 99.63% pada dataset LFW (Nemavhola, et al., 2025). *FaceNet* juga sering digunakan untuk komputasi embedding dalam berbagai sistem pengenalan wajah (Lin, et al., 2023).
3) *ResNet* (*Residual Neural Network*): Dirancang untuk mengatasi masalah vanishing gradient yang sering muncul pada jaringan yang sangat dalam. *ResNet* memperkenalkan "koneksi residual" atau *shortcut connections* yang memungkinkan gradien mengalir lebih mudah selama proses pelatihan, sehingga memungkinkan pembuatan jaringan dengan kedalaman yang jauh lebih besar dibandingkan *VGGNet* sambil tetap mempertahankan atau bahkan meningkatkan kinerja (Nemavhola, et al., 2025).
4) *MobileNet*: Merupakan keluarga arsitektur CNN yang dirancang khusus untuk efisiensi komputasi pada perangkat dengan sumber daya terbatas, seperti perangkat seluler atau *embedded* sistems. *MobileNet* menggunakan *depthwise separable convolutions* untuk mengurangi jumlah parameter dan operasi komputasi secara signifikan tanpa mengorbankan terlalu banyak akurasi (Nemavhola, et al., 2025). Varian seperti *MobileNetV3* sering disebut dalam konteks ini (Chautharia dan Bodepudi, 2024).

5) MTCNN (*Multi-Task Cascaded Convolutional Networks*): Arsitektur ini efektif untuk melakukan deteksi wajah dan deteksi landmark wajah secara bersamaan dalam satu pipeline bertingkat. MTCNN menyoroti pentingnya pendekatan multi-task learning dalam visi komputer dan telah digunakan untuk deteksi dan penyelarasan wajah berkualitas tinggi (Nemavhola, et al., 2025).
6) *ArcFace*: Memperkenalkan *additive angular margin loss* yang bertujuan untuk meningkatkan diskriminasi fitur wajah dalam ruang *embedding*. Dengan memaksimalkan margin keputusan pada *manifold hypersphere*, *ArcFace* mampu menghasilkan fitur yang lebih terpisah antar kelas (identitas) dan lebih kompak intra kelas (Lin, et al., 2023). *ArcFace* telah digunakan untuk ekstraksi fitur pada perangkat *edge* (Ozen et al., 2024).

Evolusi arsitektur CNN untuk pengenalan wajah menunjukkan sebuah tren yang menarik. Awalnya, fokus adalah pada peningkatan kedalaman dan kompleksitas untuk mencapai akurasi yang lebih tinggi. Kemudian, perhatian bergeser ke arah optimalisasi efisiensi untuk penerapan praktis pada perangkat dengan sumber daya terbatas dan pengembangan arsitektur yang dirancang untuk tugas-tugas yang lebih spesifik atau untuk mengatasi tantangan tertentu dalam pengenalan wajah. Hal ini mencerminkan kebutuhan ganda dalam pengembangan sistem pengenalan wajah: akurasi yang tinggi dan kemampuan untuk diimplementasikan secara efisien di dunia nyata.

Selain arsitektur jaringan pada CNN, inovasi dalam fungsi loss telah menjadi pendorong utama peningkatan kinerja. Ini mengindikasikan bahwa cara model belajar untuk membedakan antara wajah-wajah yang berbeda sama pentingnya dengan fitur-fitur spesifik apa yang diekstraksi oleh lapisan-lapisan konvolusi.

Pemilihan arsitektur CNN untuk sistem absensi yang diusulkan dalam penelitian ini harus secara cermat mempertimbangkan keseimbangan antara akurasi dan kecepatan pemrosesan Arsitektur seperti *MobileNet* atau varian yang lebih ringan dari *ResNet* atau *FaceNet* mungkin menjadi kandidat yang lebih sesuai. Perbandingan arsitektur CNN ditampilkan pada tabel 1.

Tabel 1. Perbandingan Arsitektur CNN untuk Pengenalan Wajah

Arsitektur	**Dataset**	**Akurasi**	**Inference**	**Kelebihan**	**Kelemahan**
VGG16	LFW, VGGFace	>98% (LFW), 98.95% (VGGFace)	Rendah / Banyak	Akurasi tinggi, arsitektur sederhana	Berat, lambat di perangkat standar
FaceNet	LFW, YouTube Faces	99.63% (LFW)	Sedang / Sedang	Embedding kuat, cocok untuk verifikasi & identifikasi	Masih cukup berat untuk beberapa skenario
ResNet50	ImageNet, LFW	Bervariasi (tinggi)	Sedang / Banyak	Deep network stabil, menangani vanishing gradient	Kompleks dan ukuran model besar
MobileNetV3	ImageNet, LFW (adaptasi)	Kompetitif	Tinggi / Sedikit	Ringan, cocok untuk perangkat mobile	Akurasi sedikit di bawah model besar
MTCNN	WIDER Face, LFW	99.85% (deteksi)	Sedang	Deteksi wajah + landmark, akurasi tinggi	Fokus pada deteksi, bukan embedding
ArcFace	LFW, MegaFace	>99% (LFW)	Sedang	Diskriminasi fitur sangat baik (angular margin loss)	Butuh loss function khusus

b. Proses Ekstraksi Fitur Wajah

Salah satu keunggulan utama CNN adalah kemampuannya untuk secara otomatis mempelajari fitur-fitur yang paling diskriminatif dari data gambar wajah mentah, tanpa memerlukan rekayasa fitur manual

yang rumit (Pavan dan Thanuja, 2023). Melalui serangkaian lapisan konvolusi dan pooling, CNN secara bertahap membangun representasi fitur yang semakin kompleks, mulai dari tepi dan tekstur sederhana hingga bagian-bagian wajah dan akhirnya representasi wajah secara keseluruhan.

Hasil akhir dari proses ekstraksi fitur ini biasanya adalah sebuah *feature vector* atau *embedding* wajah. *Embedding* ini merupakan representasi numerik yang kompak dan berdimensi rendah dari wajah input, di mana wajah-wajah yang mirip secara visual akan memiliki *embedding* yang berdekatan dalam ruang fitur, sedangkan wajah-wajah yang berbeda akan memiliki *embedding* yang berjauhan (Ray 2025). Embedding inilah yang kemudian digunakan untuk proses pencocokan atau klasifikasi identitas.

2. Landmark Detection

Landmark Detection adalah proses melokalisasi titik-titik kunci pada fitur-fitur wajah yang paling menonjol, seperti sudut mata, ujung hidung, sudut bibir, kontur alis, dan garis rahang (Meghana, et al., 2021). Landmark ini menyediakan informasi struktural penting tentang wajah dan menjadi dasar untuk berbagai aplikasi analisis wajah.

a. Teknik Deteksi Landmark Populer

Dua teknik atau pustaka yang sangat populer dan sering digunakan untuk deteksi landmark wajah adalah Dlib dan MediaPipe.

1) Dlib**:** Pustaka Dlib menyediakan model deteksi landmark wajah yang sangat dikenal, yang didasarkan pada metode ensemble of regression trees yang dipublikasikan oleh Kazemi dan Sullivan pada tahun 2014. Model ini umumnya menghasilkan 68 titik landmark 2D yang telah terbukti andal dan cepat (Zhi Jie, et al., 2023). Dlib juga menawarkan detektor wajah berbasis HOG + Linear SVM dan MMOD CNN (Chandel et al., 2023).

2) *MediaPipe Face Mesh*: Dikembangkan oleh Google, *MediaPipe Face Mesh* adalah solusi berbasis *machine learning* yang mampu mendeteksi hingga 468 *landmark* wajah dalam format 3D secara *real-time*, bahkan pada perangkat seluler (Meghana, et al., 2021). *Pipeline* ML-nya terdiri dari dua model utama: model deteksi wajah yang beroperasi pada gambar penuh, dan model *landmark* wajah yang kemudian bekerja pada *Region of Interest* (ROI) wajah yang terdeteksi (Zhi Jie, et al., 2023). Kinerja MediaPipe pada perangkat edge seperti Raspberry Pi telah dilaporkan baik dalam hal akurasi dan kecepatan (Shah, et al., 2024).

Dalam pemilihan antara Dlib dan *MediaPipe*, terdapat pertimbangan *trade-off. MediaPipe* dengan 468 *landmark* 3D menawarkan representasi wajah yang jauh lebih detail dan kaya, yang berpotensi sangat berguna untuk analisis gerakan halus atau pemodelan 3D. Di sisi lain, Dlib dengan 68 *landmark* 2D mungkin menawarkan kecepatan komputasi yang sedikit lebih tinggi dalam beberapa skenario, meskipun *MediaPipe* juga dirancang untuk efisiensi *real-time*. Kemudahan penggunaan kedua pustaka ini sangat didukung oleh ketersediaan model pra-terlatih yang kuat, yang secara signifikan mengurangi hambatan implementasi.

Untuk aplikasi deteksi keaktifan berbasis gerakan, jumlah dan akurasi landmark yang lebih tinggi dari *MediaPipe* berpotensi memungkinkan deteksi gerakan halus yang lebih baik dan lebih andal. Informasi umum Teknik deteksi *landmark* ditampilkan pada tabel 2

Tabel 2. Informasi Umum Teknik Deteksi *Landmark*

Teknik	Jumlah	Dimensi	Kecepatan	Akurasi
Dlib (68-point)	68	2D	Cepat	Baik
Mediapipe Face Mesh	468	3D	Sangat Cepat	Sangat Baik

Kelebihan dan kekurangan Teknik deteksi *Landmark* di tampilkan pada table 3.

Tabel 3. Kelebihan dan Kekurangan Teknik Deteksi *Landmark* (Lanjutan)

Teknik	Kelebihan	Kekurangan	Pustaka
Dlib (68-point)	Cepat, model pre-trained andal, banyak digunakan	Jumlah landmark terbatas, hanya 2D	Dlib (Python, C++)
MediaPipe Face Mesh	Banyak landmark, 3D, real-time di seluler, estimasi pose terintegrasi	Mungkin sedikit lebih kompleks untuk setup awal	MediaPipe (Python, JS, Android, iOS)

b. Peran *Landmark* dalam Analisis Wajah dan Deteksi Keaktifan

Deteksi landmark wajah bukan hanya tujuan akhir, tetapi juga merupakan langkah penting untuk berbagai tugas analisis wajah lainnya:

1) Penyelarasan Wajah (*Face Alignment*): *Landmark* digunakan untuk menormalkan orientasi dan skala wajah sebelum diproses lebih lanjut oleh model pengenalan, sehingga dapat meningkatkan akurasi secara signifikan (Nemavhola, et al., 2025).
2) Estimasi Pose Kepala: Posisi relatif landmark dapat digunakan untuk mengestimasi orientasi atau pose kepala (*yaw, pitch, roll*), yang penting untuk menangani variasi kemiringan wajah dalam skenario dunia nyata (Lin, et al., 2023).

3) Dasar untuk Deteksi Keaktifan Berbasis Gerakan: Perubahan posisi *landmark* dari waktu ke waktu menjadi dasar untuk mendeteksi berbagai isyarat keaktifan, seperti kedipan mata, gerakan mulut saat berbicara, gerakan kepala (anggukan atau gelengan), dan perubahan ekspresi wajah lainnya (Zhi Jie, et al., 2023).

3. Deteksi Keaktifan (*Liveness Detection*)

Deteksi keaktifan, atau *liveness detection*, adalah kemampuan sebuah sistem biometrik untuk membedakan secara andal antara subjek biometrik yang hidup dan hadir secara fisik pada saat pengambilan sampel dengan upaya pemalsuan menggunakan representasi non-hidup atau rekaman (Raj, et al., 2021). Ini adalah komponen keamanan krusial untuk mencegah serangan *spoofing* dan memastikan integritas serta kepercayaan terhadap sistem biometric (Ryando et al., 2025). bahkan menekankan bahwa deteksi keaktifan adalah pertahanan utama terhadap serangan presentasi.

a. Jenis-jenis Serangan *Spoofing* (*Presentation Attack – PAs*)

Serangan spoofing pada sistem pengenalan wajah dapat dikategorikan berdasarkan media dan metode yang digunakan:

1) Serangan Foto (2D Statis). Ini adalah jenis serangan yang paling umum dan sederhana, melibatkan penggunaan foto cetak berkualitas baik atau foto digital yang ditampilkan pada layar perangkat lain untuk menipu sensor kamera (Khairnar, et al., 2023). mengklasifikasikan ini lebih lanjut menjadi *Printed Photo Attacks, Cut Photo Attacks* (foto dengan lubang di mata untuk simulasi kedipan), dan *Wrapped Photo Attacks* (foto yang sedikit ditekuk untuk memberi kesan kedalaman).
2) Serangan Video (2D Dinamis). Serangan ini menggunakan rekaman video dari pengguna yang sah yang diputar ulang di depan kamera sistem. *Video replay attacks* lebih canggih daripada serangan foto karena dapat menampilkan beberapa dinamika wajah seperti gerakan mata atau perubahan ekspresi kecil (Padmashree dan Karunakar, 2024).

3) Serangan Topeng (3D). Melibatkan penggunaan topeng fisik untuk meniru wajah target. Ini bisa berupa topeng 2D yang fleksibel yang ditempelkan pada struktur tertentu, topeng 3D yang dicetak atau dibuat secara kaku, hingga topeng silikon berkualitas tinggi yang sangat realistis (Khairnar, et al., 2023). juga menyebutkan *Makeup Presentation Attacks* dan *Silicon Masks*.

Eskalasi jenis serangan dari yang sederhana seperti foto cetak hingga yang sangat canggih seperti injeksi video dan deepfakes menunjukkan adanya "perlombaan senjata" yang berkelanjutan antara pihak penyerang dan pengembang sistem keamanan. Hal ini mengimplikasikan bahwa tidak ada satu metode deteksi keaktifan tunggal yang mungkin efektif melawan semua jenis serangan ini. Sebagai contoh, serangan menggunakan topeng 3D mungkin memerlukan penggunaan sensor kedalaman untuk deteksi yang efektif, sementara serangan berbasis video memerlukan analisis temporal yang cermat. Untuk sistem absensi yang diusulkan, prioritas pertahanan harus diberikan terhadap jenis serangan yang paling mungkin terjadi dalam skenario tersebut, yaitu serangan foto dan *video replay* sederhana, sambil tetap menyadari dan mempersiapkan diri terhadap potensi ancaman yang lebih canggih di masa depan.

b. Metode *Liveness Detection* Umum

Berbagai pendekatan telah dikembangkan untuk *Liveness Detection*, masing-masing dengan prinsip kerja, kelebihan, dan kekurangannya sendiri:

1) Berbasis Tekstur (*Texture-based*). Metode ini menganalisis detail tekstur halus pada permukaan kulit wajah yang diharapkan berbeda secara signifikan antara wajah manusia asli dan artefak palsu. Misalnya, foto cetak mungkin memiliki pola titik-titik

printer, sedangkan tampilan layar mungkin menunjukkan pola moiré. Teknik umum yang digunakan meliputi *Local Binary Patterns (LBP)* dan *Histogram of Oriented Gradients (HOG)* (Ryando et al. 2025). Pendekatan ini cenderung efektif untuk serangan statis (Khairnar, et al., 2023)

2) Berbasis Gerakan (*Motion-based*). Menganalisis gerakan alami yang dihasilkan oleh wajah hidup, seperti kedipan mata, gerakan bibir saat berbicara, gerakan kepala dan perubahan ekspresi wajah (Ryando et al., 2025). membagi ini lebih lanjut menjadi metode berbasis Interaksi Manusia-Komputer (HCI) yang memerlukan tindakan spesifik dari pengguna, dan metode berbasis informasi kehidupan.
3) Berbasis Kedalaman (*Depth-based*). Memanfaatkan informasi tiga dimensi (3D) dari wajah. Wajah manusia asli memiliki struktur kedalaman yang kompleks, sedangkan foto atau video yang ditampilkan pada permukaan datar bersifat 2D. Informasi kedalaman dapat diperoleh dari sensor khusus atau diestimasi dari gambar 2D menggunakan teknik tertentu (Ryando et al., 2025). Namun, metode ini seringkali memerlukan perangkat keras tambahan atau mahal (Khairnar, et al., 2023), dan bahkan informasi kedalaman pun dapat dipalsukan melalui serangan seperti *DepthFake* (Wu, et al., 2023).
4) Berbasis Fokus/Defokus Gambar (*Image Focus/Defocus-based*). Teknik ini memanfaatkan perbedaan tingkat keburaman (blur) antara berbagai bagian wajah yang timbul karena efek *Depth of Field (DoF)* pada kamera saat memotret objek 3D. Perbedaan ini tidak akan signifikan pada objek 2D seperti foto (Wu et al., 2023). Berapa metode mengambil dua gambar secara berurutan dengan pengaturan fokus yang berbeda untuk menganalisis perubahan ini (Wu et al., 2023).

5) Berbasis Tantangan-Respons (*Challenge-Response*). Sistem secara aktif meminta pengguna untuk melakukan serangkaian tindakan atau respons acak tertentu, seperti tersenyum, mengangguk, menggelengkan kepala, mengikuti objek yang bergerak di layar, atau mengucapkan frasa tertentu. Keberhasilan atau kegagalan pengguna dalam merespons tantangan ini dengan benar dan alami digunakan untuk memverifikasi keaktifan (Kamarowski et al., 2023). memberikan klasifikasi detail metode ini.
6) Berbasis Kualitas Gambar (*Image Quality Assessment - IQA*). Mendeteksi berbagai artefak visual yang sering muncul pada gambar atau video hasil spoofing, seperti distorsi warna, tingkat noise yang tidak biasa, keburaman yang tidak wajar, atau pola aneh lainnya yang tidak ada pada tangkapan kamera langsung dari wajah asli (Khairnar, et al., 2023).
7) Pendekatan Berbasis *Deep Learning*. Menggunakan arsitektur jaringan saraf tiruan dalam seperti CNN atau *Recurrent Neural Networks (RNN/LSTM)* untuk secara otomatis mempelajari fitur-fitur pembeda antara wajah asli dan wajah palsu dari dataset besar yang berisi contoh kedua jenis tersebut (Raj, et al., 2021). Arsitektur CNN-LSTM sering digunakan untuk analisis video (Koshy dan Mahmood, 2020).

Dalam memilih metode deteksi keaktifan, terdapat spektrum dari yang pasif dan non-intrusif hingga yang aktif dan berpotensi intrusif bagi pengguna (misalnya, *challenge-response*). Untuk aplikasi sistem absensi, metode yang lebih pasif, cepat, dan tidak memerlukan interaksi pengguna yang rumit umumnya lebih disukai. Beberapa metode, seperti yang berbasis kedalaman atau fokus tertentu, mungkin juga bergantung pada ketersediaan perangkat keras kamera khusus atau kemampuan kontrol fokus yang tidak selalu ada pada perangkat standar.

Eye Aspect Ratio (EAR) merupakan ukuran yang digunakan untuk mendeteksi perubahan pada mata, khususnya kedipan. EAR dihitung dengan perbandingan jarak *vertikal* dan *horizontal* mata menggunakan *facial landmark*. Nilai EAR akan menurun secara signifikan ketika mata berkedip.

$$EAR = \frac{\left||p_2 - p_6|\right| + ||p_3 - p_5||}{2 \times |p_1 + p_4|}$$

Mouth Aspect Ratio (MAR) digunakan untuk mengukur pergerakan mulut. MAR dihitung dari perbandingan jarak vertikal dengan jarak horizontal bibir. Nilai MAR meningkat ketika mulut terbuka.

$$MAR = \frac{\left||p_{14} - p_{18}|\right| + ||p_{13} - p_{19}|| + ||p_{12} + p_{20}||}{2 \times |p_{11} + p_{17}|}$$

Keterangan p_i merepresentasikan titik facial landmark pada mata dan mulut sesuai indeks yang ditetapkan oleh *MediaPipe*.

Kemampuan deep learning untuk mempelajari fitur secara otomatis dari data menjadikannya pendekatan yang sangat menjanjikan dan fleksibel, terutama ketika dikombinasikan dengan isyarat spesifik seperti gerakan landmark atau analisis temporal untuk video. Pilihan metode *liveness Detection* untuk penelitian ini harus selaras dengan batasan perangkat keras yang diantisipasi (kamera RGB standar) dan jenis serangan utama yang ingin dicegah, dengan fokus pada metode yang dapat diimplementasikan secara efektif menggunakan data *landmark* wajah.

Dengan mempertimbangkan efisiensi dan kenyamanan pengguna, pendekatan berbasis analisis pergerakan alami wajah melalui *landmark* menjadi pilihan yang ideal. Selain tidak memerlukan perangkat keras tambahan, pendekatan ini mampu mendeteksi tanda-tanda kehidupan secara halus dan real-time, serta

dapat diintegrasikan langsung dengan modul deteksi wajah yang telah ada dalam sistem. Prinsip dasar dan kelebihan metode deteksi serangan wajah ditampilkan pada tabel 4.

Tabel 4. Prinsip Dasar dan Kelebihan Metode Deteksi Serangan Wajah

Metode	**Prinsip Dasar**	**Kelebihan**
Tekstur (LBP, HOG)	Analisis pola tekstur mikro pada permukaan wajah.	Cepat, komputasi ringan, baik untuk serangan foto.
Kedalaman (Depth-based)	Pemanfaatan informasi 3D wajah.	Sangat efektif jika data kedalaman akurat.
Kualitas Gambar (IQA)	Deteksi artefak (distorsi, noise) pada media palsu.	Cepat, non-intrusif.
Deep Learning (Umum)	Pembelajaran fitur otomatis dari data besar.	Adaptif, kinerja state-of-the-art.

Kekurangan dan tantangan metode deteksi serangan wajah ada pada tabel 5.

Tabel 5. Kekurangan dan Tantangan Metode

Metode	**Kekurangan / Tantangan**
Tekstur (LBP, HOG)	Rentan terhadap pencahayaan, kualitas cetak; kurang efektif untuk video.
Kedalaman (Depth-based)	Butuh sensor mahal, bisa dipalsukan (*DepthFake*).
Kualitas Gambar (IQA)	Rentan jika spoof sangat tinggi.
Deep Learning (Umum)	Butuh banyak data, bersifat black box, pelatihan komputasi tinggi.

Efektivitas terhadap serangan dan kebutuhan perangkat khusus ditampilkan pada tabel 6.

Tabel 6. Efektivitas terhadap Serangan dan Kebutuhan Perangkat khusus

Metode	**Efektivitas Serangan (Foto, Video, Topeng)**	**Perangkat Keras Khusus**
Tekstur (LBP, HOG)	Baik, Sedang, Kurang	Tidak
Kedalaman (Depth-based)	Baik, Baik, Sangat Baik	Ya (Sensor Kedalaman)
Kualitas Gambar (IQA)	Sedang, Sedang, Kurang	Tidak
Deep Learning (Umum)	Baik–Sangat Baik (tergantung arsitektur & data)	Tidak (umumnya)

c. Deteksi Keaktifan Berbasis Gerakan *Landmark*

Salah satu pendekatan yang menjanjikan dan relevan untuk penelitian ini adalah deteksi keaktifan yang berbasis pada analisis gerakan dinamis dari *landmark* wajah. Prinsip dasarnya adalah bahwa wajah manusia asli yang hidup akan selalu menunjukkan pola gerakan mikro dan makro yang konsisten pada landmark-nya, seperti kedipan mata yang tidak disadari, gerakan bibir saat berbicara atau bahkan saat diam, sedikit gerakan kepala, dan perubahan ekspresi wajah yang halus. Gerakan-gerakan alami ini sulit untuk ditiru secara sempurna dan konsisten oleh serangan spoofing statis (foto) atau bahkan oleh video replay sederhana (Zhi Jie, et al., 2023).

Beberapa contoh implementasi deteksi keaktifan berbasis gerakan landmark meliputi:

1) Deteksi Kedipan Mata, dapat dilakukan dengan menganalisis perubahan jarak vertikal antara landmark kelopak mata atas dan bawah. Metrik seperti *Eye Aspect Ratio (EAR)* sering digunakan untuk mengukur tingkat keterbukaan mata (Ali et al., 2023). Pola perubahan EAR dari waktu ke waktu dapat mengindikasikan kedipan mata yang alami (dengan durasi dan frekuensi tertentu), yang akan berbeda dari mata yang statis pada foto atau gerakan mata yang tidak alami pada video replay (Ryando et al., 2025). Model CNN kecil bahkan dapat dilatih khusus untuk klasifikasi kedipan mata dari ROI mata atau dari urutan nilai EAR (Zhi Jie, et al., 2023).
2) Deteksi Gerakan Mulut, perubahan jarak dan bentuk landmark bibir dapat dianalisis. Misalnya, *Mouth Aspect Ratio (MAR)* dapat dihitung untuk mendeteksi apakah mulut terbuka atau tertutup, atau untuk menganalisis pola gerakan bibir saat berbicara (Zhi Jie, et al., 2023).
3) Deteksi Gerakan Kepala, perubahan posisi relatif dari landmark sentral wajah atau perubahan orientasi wajah secara keseluruhan dapat digunakan untuk mendeteksi gerakan kepala seperti anggukan atau gelengan (Zhi Jie, et al., 2023). MediaPipe Face Mesh, misalnya, menyediakan estimasi pose kepala 3D yang dapat dimanfaatkan untuk ini (Meghana, et al., 2021).
4) Analisis Ekspresi, perubahan ekspresi wajah, seperti tersenyum, dapat dideteksi berdasarkan pergerakan kombinasi landmark di sekitar mulut dan mata (Zhi Jie, et al., 2023). Ini bisa menjadi bagian dari mekanisme challenge-response implisit atau sebagai salah satu isyarat keaktifan pasif.

Penggunaan teknik *machine learning* atau *deep learning* sangat relevan di sini untuk mempelajari pola gerakan landmark yang normal dan membedakannya dari pola yang abnormal atau palsu (Zhi Jie, et al., 2023). Landmark wajah menyediakan data spasial dan temporal yang kaya, yang dapat dieksploitasi untuk deteksi keaktifan yang lebih halus dan andal dibandingkan dengan analisis frame tunggal atau fitur global. Menggabungkan analisis beberapa jenis gerakan *landmark* berpotensi meningkatkan robustisitas deteksi keaktifan secara signifikan.

Namun, tantangan tetap ada dalam membedakan gerakan alami dari gerakan yang mungkin disengaja oleh penyerang untuk menipu sistem, atau dari artefak gerakan yang mungkin ada pada rekaman video berkualitas rendah.

d. Teknik *Anti-Spoofing Video*

Mengingat serangan *video replay* merupakan ancaman yang signifikan, beberapa teknik khusus dapat dipertimbangkan untuk melawannya.

1) Analisis Temporal, menganalisis konsistensi dan dinamika fitur wajah atau *landmark* wajah sepanjang urutan frame video. Serangan *video replay* mungkin menunjukkan pola temporal yang tidak alami, seperti gerakan yang terlalu mulus atau terlalu kaku, pengulangan pola, atau artefak transisi antar frame yang tidak wajar (Khairnar et al., 2023). Penggunaan arsitektur CNN-LSTM, di mana CNN mengekstrak fitur spasial per frame dan LSTM memodelkan dependensi temporal antar frame, adalah pendekatan yang umum untuk klasifikasi video sebagai asli atau palsu (Koshy and Mahmood 2020).
2) Analisis Tekstur Frame, mencari artefak visual yang spesifik terkait dengan proses perekaman ulang dari layar, seperti pola moiré (garis-garis interferensi yang muncul saat memfoto atau

merekam layar digital), distorsi warna, atau kualitas fokus yang seragam secara tidak alami di seluruh area wajah (Khairnar, et al., 2023).

3) Deteksi Injeksi Video, ini adalah mekanisme pertahanan yang lebih canggih yang bertujuan untuk mendeteksi apakah input video yang diterima sistem berasal dari kamera virtual, file video yang dimanipulasi, atau sumber lain yang bukan merupakan tangkapan langsung dari kamera fisik perangkat. *FaceTec* adalah salah satu vendor yang secara khusus mengklaim menangani jenis serangan ini.
4) Analisis Cahaya dan Bayangan, wajah manusia asli yang bersifat 3D akan berinteraksi dengan pencahayaan lingkungan secara dinamis dan menghasilkan pola bayangan yang konsisten dengan bentuknya. Gambar 2D yang diputar ulang di layar datar mungkin tidak menunjukkan interaksi cahaya dan bayangan yang sama, terutama jika ada perubahan pada pencahayaan sekitar

Untuk sistem absensi, serangan *video replay* merupakan ancaman yang lebih canggih dan berpotensi lebih umum daripada, misalnya, topeng 3D berkualitas tinggi. Oleh karena itu, fokus pada teknik *anti-spoofing video* sangatlah penting. Kemungkinan besar, strategi *anti-spoofing video* yang efektif akan memerlukan kombinasi beberapa jenis petunjuk (misalnya, analisis gerakan landmark secara temporal, ditambah dengan analisis tekstur frame) karena penyerang mungkin dapat menemukan cara untuk mengatasi satu jenis mekanisme deteksi saja. Dalam konteks penelitian ini, analisis gerakan *landmark* secara adalah kandidat yang kuat dan relevan.

4. Penanganan Variasi Pose dan Kemiringan Wajah

Variasi pose atau kemiringan wajah merupakan salah satu tantangan utama dalam sistem pengenalan wajah yang beroperasi di lingkungan dunia nyata yang tidak terkontrol (Nemavhola et al., 2025). Perubahan sudut pandang wajah dapat secara drastis mengubah penampilan fitur wajah, sehingga menyulitkan model untuk melakukan pencocokan yang akurat (Kasture et al., 2025), misalnya, menunjukkan penurunan akurasi untuk deteksi wajah dari samping.

Beberapa pendekatan umum untuk mencapai invariansi atau toleransi terhadap variasi pose meliputi:

a. Normalisasi Pose berbasis *Landmark*, menggunakan lokasi landmark wajah yang terdeteksi untuk melakukan transformasi geometris pada gambar wajah. Tujuannya adalah untuk menormalkan wajah ke tampilan frontal atau semi-frontal sebelum fitur diekstraksi oleh CNN (Lin et al., 2023). Ini membantu mengurangi variasi input yang diterima oleh model pengenalan.
b. Ekstraksi Fitur yang Robust terhadap Pose, menggunakan arsitektur CNN yang telah dilatih dengan dataset yang sangat beragam dan mencakup berbagai macam pose wajah. Teknik augmentasi data dengan variasi pose juga sangat penting di sini. Beberapa arsitektur mungkin secara inheren lebih baik dalam menangani variasi pose karena desainnya.
c. *Ensemble Learning* dengan Deskriptor Fitur Lokal, pendekatan ini melibatkan pelatihan beberapa model *base learner* yang masing-masing fokus pada vektor fitur yang diekstraksi dari daerah di sekitar landmark wajah tertentu. Keputusan akhir kemudian diambil dengan menggabungkan *output* dari *base learner* yang relevan. Penelitian oleh Lin et al., (2023) menyajikan pendekatan semacam ini yang mampu menangani variasi pose hingga ±90° dengan menggunakan Face *Angle Vector (FAV)* untuk klasifikasi pose dan *Base Learner Selection (BLS)* untuk memilih base learner yang paling sesuai.

d. Model 3D, beberapa metode mencoba merekonstruksi model wajah 3D dari satu atau beberapa gambar 2D. Setelah model 3D diperoleh, tampilan wajah dari sudut pandang frontal (atau sudut pandang standar lainnya) dapat disintesis secara virtual (Lin, et al., 2023). Penggunaan *3D Morphable Model (3DMM)* adalah salah satu contohnya, (Lin et al., 2023).

Deteksi landmark wajah yang akurat adalah prasyarat penting untuk banyak teknik penanganan variasi pose, terutama untuk metode normalisasi pose dan pendekatan berbasis fitur lokal. Metode yang lebih canggih seperti pemodelan 3D atau *ensemble learning* yang kompleks mungkin menawarkan toleransi pose terbaik, tetapi seringkali datang dengan biaya komputasi yang lebih tinggi. Untuk aplikasi sistem absensi, perlu ditemukan keseimbangan antara tingkat toleransi pose yang diinginkan dan efisiensi komputasi.

Dalam arsitektur sistem yang diusulkan, modul deteksi landmark harus dieksekusi sebelum atau setidaknya bersamaan dengan tahap ekstraksi fitur utama jika normalisasi pose akan diterapkan sebagai salah satu strategi penanganan variasi pose.

B. Penelitian Terkait

Beberapa penelitian sebelumnya telah mengeksplorasi integrasi teknologi seperti CNN, deteksi *landmark* wajah, dan deteksi keaktifan (*liveness detection*) untuk membangun sistem pengenalan wajah atau sistem absensi yang lebih aman dan akurat.

Sebagai contoh, penelitian oleh Zhi Jie, Tong Ming, dan Chi Wee (2023) menggabungkan deteksi *landmark* menggunakan MediaPipe dan Dlib dengan model CNN berbasis *TensorFlow*, yang digunakan untuk mengenali gerakan mikro wajah seperti kedipan dan gerakan kepala. Penelitian oleh Koshy dan Mahmood (2020) mengusulkan pendekatan *liveness detection* berbasis gerakan menggunakan CNN-*Inception* v4 dan CNN-LSTM, yang

mampu membedakan antara wajah asli dan serangan gambar statis maupun video. Sementara itu, (Raj et al., 2021)mengembangkan sistem absensi berbasis wajah dengan kombinasi *Haar Cascade* untuk deteksi wajah, LBPH untuk pengenalan identitas, dan CNN untuk pendeteksian keaktifan pengguna.

Dalam konteks keamanan sistem pengenalan wajah, Li et al., (2022) mengusulkan pendekatan *hybrid* berbasis *optical flow* dan analisis tekstur, yang menunjukkan kinerja tinggi dalam mendeteksi serangan presentasi berbasis foto dan video. Adapun pendekatan berbasis analisis gerakan mikro wajah dalam sistem absensi juga diteliti oleh Meghana, Vasavi, dan Shravani (2021) yang menunjukkan efektivitas dalam mengidentifikasi aktivitas pengguna secara *real-time*. Terakhir, (Nemavhola et al., 2025) melakukan tinjauan literatur mendalam terhadap berbagai arsitektur CNN dalam pengenalan wajah dan menekankan pentingnya integrasi dengan metode tambahan seperti deteksi keaktifan.

Dengan menggabungkan berbagai pendekatan yang telah diteliti sebelumnya, sistem absensi berbasis pengenalan wajah dapat dikembangkan secara lebih komprehensif untuk mencapai tingkat keamanan dan akurasi yang lebih tinggi. Integrasi antara CNN, deteksi landmark, dan liveness detection tidak hanya memperkuat validasi kehadiran pengguna, tetapi juga mampu meminimalisir potensi kecurangan, seperti penggunaan foto atau video untuk meniru identitas pengguna.

Rangkuman beberapa penelitian terkait ditampilkan pada tabel 7.

Tabel 7. Penelitian Terkait

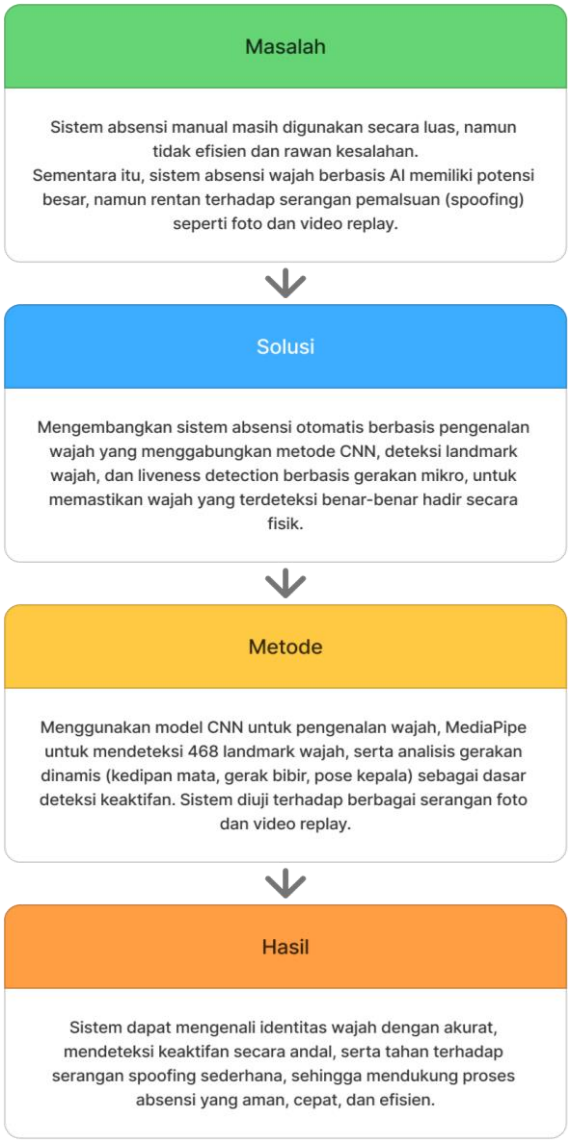
Peneliti	**Tujuan/kasus**	**Metode**	**Hasil**
(Li, et al., 2022)	Mendeteksi *spoofing* wajah menggunakan	LBP, *Optical Flow*	Mencapai akurasi 96,4% pada serangan berbasis

	pendekatan *hybrid texture + motion detection*.		foto dan video sederhana.
(Koshy dan Mahmood, 2020)	Meneliti efektivitas *eye-blink detection* dalam mendeteksi keaktifan wajah terhadap *spoofing* statis.	*Eye blink detection* + CNN	Deteksi berhasil membedakan wajah asli dan gambar diam dengan akurasi >93%
(Raj, et al., 2021)	Mengembangkan sistem absensi biometrik yang tahan terhadap serangan *spoofing*.	CNN + Liveness Detection	Sistem *hybrid* lebih unggul daripada metode CNN murni dalam menghindari absensi palsu.
(Zhi Jie, et al., 2023)	Meningkatkan akurasi deteksi wajah dengan memanfaatkan *landmark* wajah secara *real-time*.	*MediaPipe Face Mesh + Deep Learning*	Pendeteksian titik wajah akurat dan *real-time*, cocok untuk perangkat *low-end*.
(Meghana, et al., 2021)	Mengkaji performa integrasi *liveness detection* berbasis gerakan wajah (blink, bibir, kepala)	*Landmark-based motion* + CNN	Metode gerakan mikro mampu menangkal sebagian besar *spoof* berbasis video.

	dengan sistem pengenalan wajah.		
(Nemavhola, et al., 2025)	Review arsitektur CNN dalam pengenalan wajah modern.	Studi literatur CNN	CNN tetap unggul untuk pengenalan identitas, namun rentan terhadap serangan *spoofing* jika tidak digabungkan dengan metode keamanan tambahan.

C. Kerangka Berpikir

Kerangka berfikir merupakan model konseptual tentang bagaimana teori berhubungan dengan berbagai factor yang telah diidentifikasi masalah yang penting. Ilustrasi kerangka pikir penelitian ini dapat dilihat pada gambar 2.



Gambar 2. Kerangka Berpikir

BAB III

METODE PENELITIAN

A. Tempat dan Waktu Penelitian

Penelitian ini dilaksanakan di Laboratorium Informatika, Fakultas Teknik, Universitas Muhammadiyah Makassar. Proses penelitian, mulai dari studi literatur mendalam, pengumpulan dan persiapan data, perancangan dan implementasi modul-modul sistem, integrasi, hingga pengujian menyeluruh dan analisis hasil, direncanakan akan berlangsung selama periode 2 bulan. Rincian alokasi waktu untuk setiap tahapan akan mengikuti jadwal penelitian yang telah disusun. Jadwal waktu penelitian ditampilkan pada tabel 8.

Tabel 8. Waktu Penelitian

No.	Kegiatan	M1	M2	M3	M4	M5	M6	M7	M8
1	Studi Literatur dan Perumusan Masalah								
2	Perancangan Sistem dan Desain Arsitektur								
3	Implementasi Sistem (Coding)								
4	Pengujian Sistem dan Evaluasi								
5	Analisis Data dan Penyusunan Hasil Penelitian								
6	Revisi, Penyusunan Laporan Akhir								

B. Alat dan Bahan

Adapun alat dan bahan yang akan di gunakan dalam penelitian ini, yaitu :

1. Kebutuhan *Hardware* (Perangkat Keras)
    a. Laptop Hp Pavilion x360 *Convertible*
    b. *WebCam* standar (terintegrasi pada laptop)
2. Kebutuhan *Sofware* (Perangkat Lunak)

a. Sistem Operasi: Windows
b. Lingkungan Pengembangan: *Visual Studio Code*
c. Bahasa Pemograman: *Python* akan menjadi bahasa pemrograman utama
d. Pustaka Utama:
    1) *OpenCv* digunakan ntuk tugas-tugas visi komputer dasar seperti akuisisi gambar/video, pra-pemrosesan, dan beberapa fungsi deteksi.
    2) *MediaPipe* sebagai pilihan utama untuk deteksi wajah dan landmark wajah (model Face Mesh 468-titik 3D) serta estimasi pose.
    3) *Numpy* untuk manipulasi data numerik, analisis data, dan visualisasi hasil.
    4) *TensorFlow* atau *PyTorch* sebagai framework deep learning utama untuk merancang, melatih, dan mengimplementasikan model CNN untuk pengenalan wajah dan modul deteksi keaktifan.

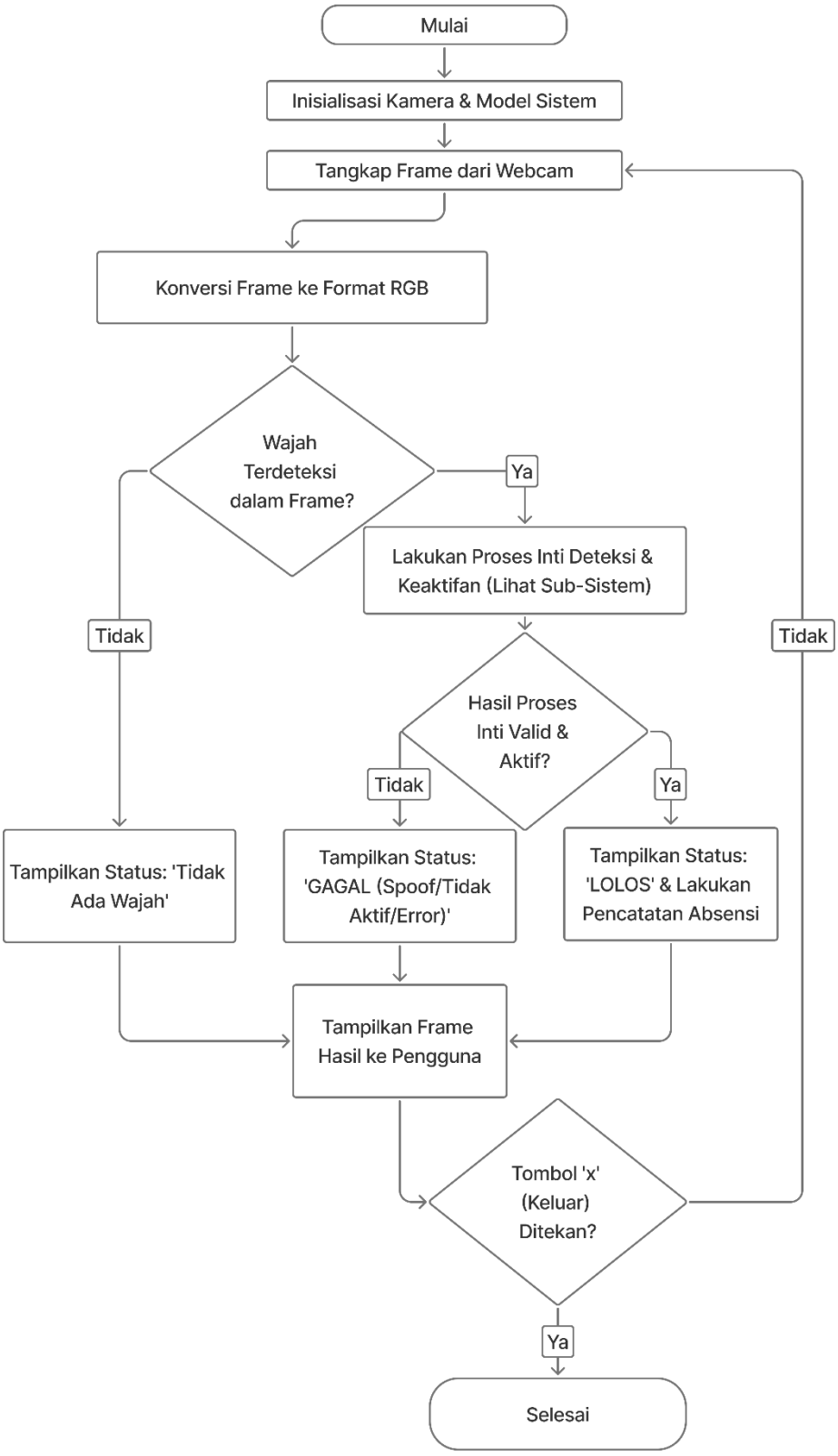
C. Perancangan Sistem

Perancangan sistem absensi pengenalan wajah ini mengadopsi pendekatan *hybrid* yang mengintegrasikan beberapa modul utama untuk mencapai akurasi dan keamanan tinggi. Sistem akan di rancang untuk beroperasi secara *real-time* menggunakan input dari *webcam*.

Arssitektur sistem secara umum diilustrasikan dalam Diagram Sistem Utama atau biasa disebut *flowchart* Gambar 3, yang menunjukkan alur kerja tingkat tinggi. Proses-proses yang lebih kompleks, khususnya terkait deteksi wajah dan keaktifan, dirinci lebih lanjut dalam sub-diagram.

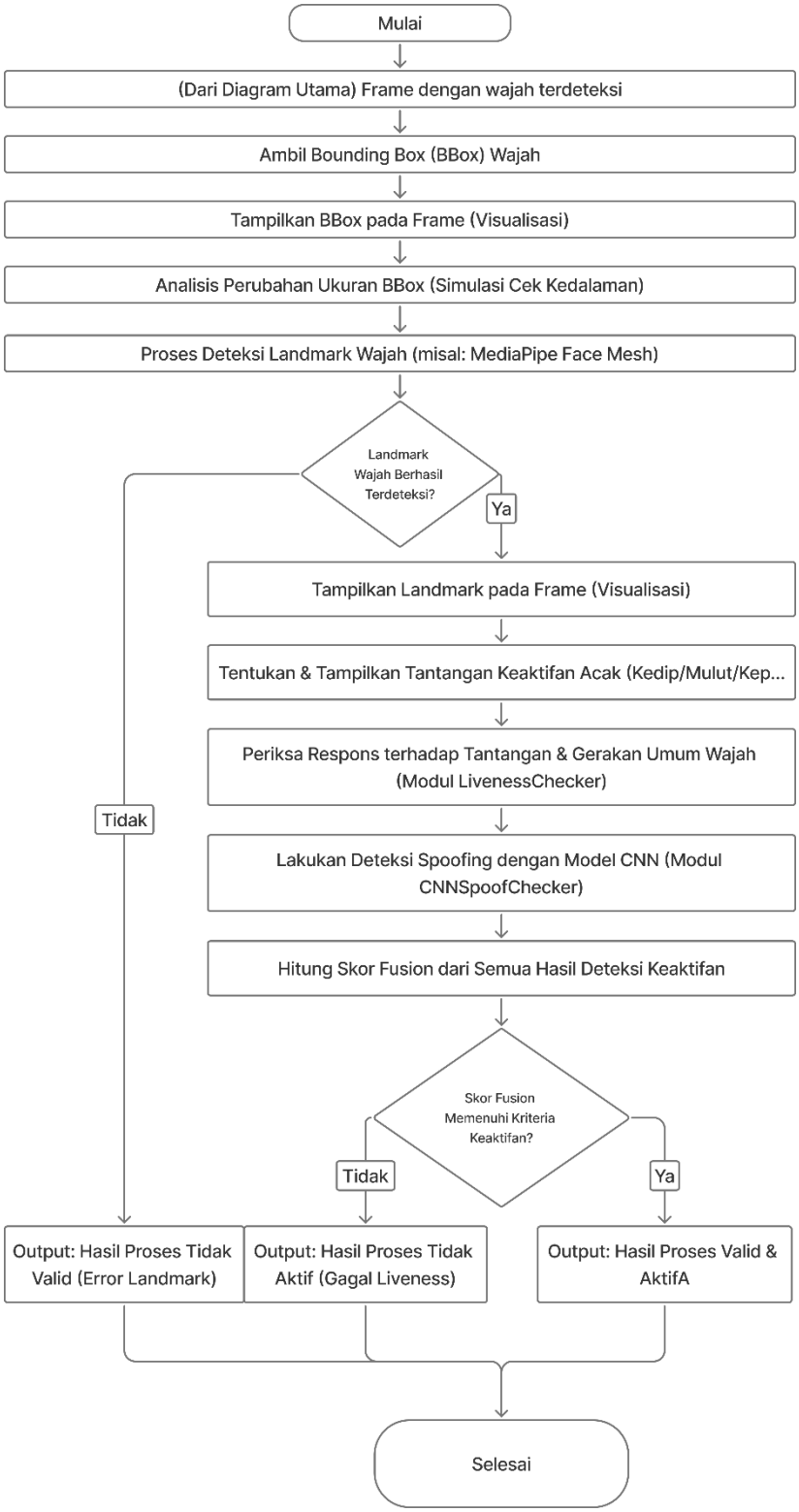
Pendekatan modular ini tidak hanya memudahkan pengembangan dan pemeliharaan sistem, tetapi juga memungkinkan fleksibilitas dalam melakukan pembaruan atau peningkatan pada komponen tertentu, seperti mengganti model CNN atau metode deteksi keaktifan.

Flowchart utama sistem ditampilkan pada gambar 3.



Gambar 3. *Flowchart* utama sistem

Flowchart sub-sistem utama pada gambar 3.



Gambar 4. *Flowchart* Sub-sistem utama

Modul-modul Utama Sistem:

1. **Akuisisi Gambar**
   a) Modul ini bertanggung jawab untuk menangkap aliran video secara kontinu dari perangkat webcam. Pustaka seperti *OpenCV* akan dipertimbangkan untuk tugas ini.
2. **Deteksi Wajah (*Face Detection*)**
   a) Sebuah model deteksi wajah yang efisien untuk aplikasi *real-time*, misalnya, yang tersedia dalam pustaka *MediaPipe*, akan digunakan untuk melokalisasi keberadaan wajah dalam setiap frame video. Detektor akan dikonfigurasi untuk optimal mendeteksi wajah dalam skenario absensi pada umumnya.
   b) Area wajah yang terdeteksi (*bounding box*) akan menjadi fokus untuk tahap pemrosesan selanjutnya, sebagaimana dirinci dalam langkah awal Sub-sistem utama.
3. **Deteksi *Landmark* Wajah (*Facial Landmark Detection*)**
   a) Setelah wajah terdeteksi, modul deteksi *landmark* wajah akan mengidentifikasi titik-titik penting pada struktur wajah. Pustaka *MediaPipe Face Mesh* menjadi kandidat utama.
   b) Informasi *landmark* ini sangat krusial untuk analisis gerakan wajah yang mendetail dan implementasi *mekanisme challenge-response*, yang merupakan bagian inti dari Sub-sistem utama.
4. **Deteksi Keaktifan (*Liveness Detection*)**

   Komponen ini dirancang secara *hybrid* untuk meningkatkan ketahanan terhadap berbagai upaya pemalsuan. Alur kerja detail dari modul deteksi keaktifan terintegrasi dalam Sub-sistem utama dan mencakup beberapa Teknik:

   a. Analisis Perubahan *Bounding Box*, teknik ini menganalisis perubahan ukuran atau skala *bounding box*

wajah antar *frame* sebagai *heuristik* sederhana untuk mendeteksi gerakan alami pengguna.

b. *Challenge-Response* Berbasis *Landmark*, Sistem akan secara dinamis memberikan tantangan kepada pengguna (misalnya, kedipan mata, gerakan mulut). Verifikasi respons akan dilakukan dengan menganalisis perubahan posisi *landmark* wajah yang relevan.

c. Deteksi Gerakan Umum Wajah, dapat menganalisis gerakan mikro atau perubahan posisi keseluruhan *landmark* wajah antar frame akan diimplementasikan untuk mendeteksi keaktifan dasar.

d. Modul Deteksi *Spoofing* Berbasis CNN, direncanakan penggunaan model *Convolutional Neural Network* (CNN) yang secara spesifik dilatih untuk membedakan antara wajah asli dan berbagai jenis artefak *spoofing*.

5. Pengenalan Wajah (CNN-*Implisit*/Potensial

a) Setelah keaktifan wajah terverifikasi (berdasarkan hasil dari Sub-sistem utama), modul pengenalan wajah dapat bertugas untuk mengidentifikasi individu. Ini akan melibatkan penggunaan arsitektur CNN untuk mengekstraksi *embedding* wajah. Fokus utama proposal ini adalah pada mekanisme *liveness detection*, namun arsitektur dirancang untuk dapat mengakomodasi modul ini.

6. Mekanisme *Fusion* dan Pengambilan Keputusan

a) Keputusan akhir mengenai apakah wajah yang dipresentasikan adalah wajah manusia asli yang hidup akan diambil berdasarkan mekanisme *fusion*, seperti yang digambarkan di akhir Sub-sistem utama. Mekanisme ini akan menggabungkan skor atau *output* dari berbagai modul deteksi keaktifan. Hasil dari *fusion* ini (valid/tidak valid, aktif/tidak aktif) akan menjadi *output* dari "Proses Inti Deteksi & Keaktifan" yang kemudian digunakan

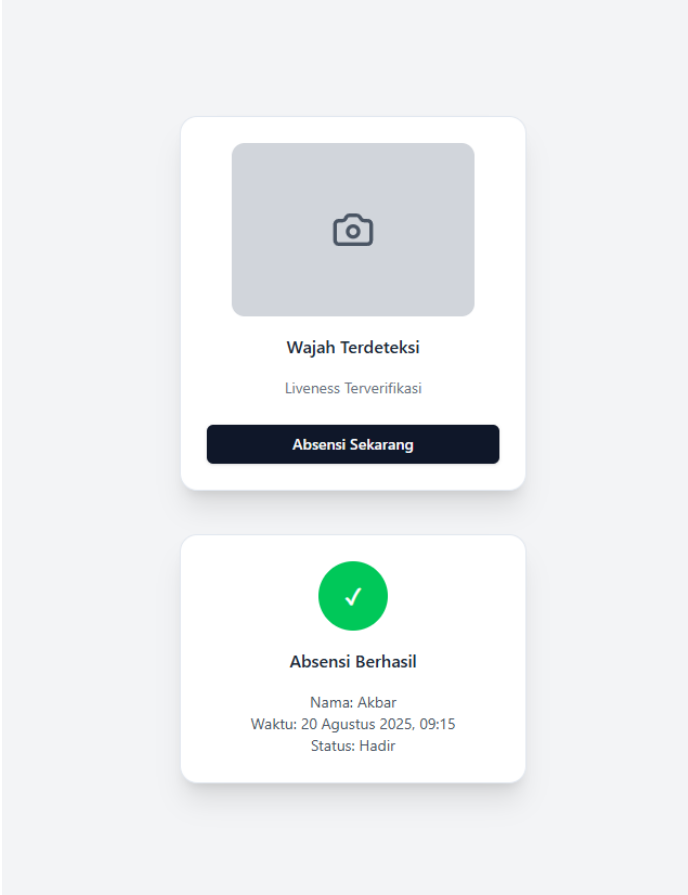
dalam Diagram Alur Utama untuk menentukan langkah selanjutnya.

7. **Pencatatan Absensi**

a) Jika sistem memverifikasi bahwa wajah yang dipresentasikan adalah asli dan hidup (berdasarkan keputusan dari Diagram Alir Utama setelah mengevaluasi *output* dari Sub-sistem utama), dan jika modul pengenalan diaktifkan dan berhasil mengidentifikasi pengguna, maka data absensi akan dicatat.

D. Desain Antarmuka Pengguna

Desain antarmuka pengguna dibuat untuk memberikan gambaran awal mengenai tampilan sistem absensi wajah yang dikembangkan. Pada tahap ini, rancangan yang disusun masih bersifat sementara dan dapat mengalami perubahan di tahap pengembangan berikutnya.



Gambar 5 Contoh MockUp awal UI

E. Teknik Pengujian Sistem

Pengujian sistem akan dilakukan untuk menilai keandalan, keamanan, dan performa dari sistem absensi yang dikembangkan. Rencana pengujian mencakup:

1. **Pengujian Fungsionalitas**
    a. Tujuannya adalah untuk memastikan sistem dapat mendeteksi wajah, *landmark*, dan *challenge* dengan benar..
    b. Metodenya dilakukan dengan menguji sistem menggunakan berbagai ekspresi wajah, variasi gerakan, dan posisi kepala.
2. **Pengujian Keamanan (*Anti-Spoofing*)**
    a. Tujuannya adalah menguji kemampuan sistem dalam mendeteksi dan menolak serangan *spoofing*, seperti penggunaan foto, layar HP, maupun video *replay*.Metode: Simulasi serangan menggunakan foto cetak, tampilan layar, dan rekaman video.
    b. Metodenya dilakukan dengan mensimulasikan serangan menggunakan foto cetak, tampilan layar, dan rekaman video.
3. **Pengujian Waktu Respons**
    a. Tujuannya adalah menilai seberapa cepat sistem memproses input hingga menghasilkan keputusan absensi.
    b. Metodenya dilakukan dengan mengukur waktu dari deteksi wajah hingga keluarnya keputusan absensi.
4. **Pengujian Stabilitas**
    a. Tujuannya adalah menilai kestabilan performa sistem pada berbagai kondisi pencahayaan dan posisi kamera.
    b. Metodenya dilakukan dengan menguji sistem pada kondisi pencahayaan terang, redup, serta variasi posisi kamera.

F. Teknik Analisis Data

Data dari hasil pengujian sistem akan dianalisis secara kuantitatif untuk menilai keakuratan, keamanan, dan performa sistem absensi yang dikembangkan. Metode analisis meliputi:

1. Keakuratan dalam system untuk menghitung persentase keberhasilan deteksi wajah, deteksi keaktifan, dan pencegahan *spoofing* dari jumlah total percobaan.
2. ***False*** *Acceptance Rate* (FAR) dan *False Rejection Rate* (FRR) untuk mengukur kemampuan sistem dalam membedakan wajah asli dan serangan *spoofing*.
3. Kecepatan Sistem untuk Mengukur rata-rata waktu deteksi dan pengambilan keputusan sistem. Data hasil pengujian akan ditabulasikan dan divisualisasikan dalam bentuk tabel atau grafik untuk mempermudah interpretasi hasil pada laporan akhir.

DAFTAR PUSTAKA

Ali, Shahad Salh, Jamila Harbi Al'ameri, and Thekra Abbas. 2023. 'Real Time E-Learning Students Monitoring for Optimization Facial Landmark Recognition Based on Hybrid Deep Learning Techniques'. *Journal of Intelligent Systems and Internet of Things* 10(2):102–12. doi:10.54216/JISIoT.100209.

Chandel, Ritika, Rajnandini Bhowmick, and U. Hariharan. 2023. 'A Comparison of Face Landmark Detection Techniques'. in *2023 4th International Conference on Computation, Automation and Knowledge Management, ICCAKM 2023*. Institute of Electrical and Electronics Engineers Inc.

Chautharia, Jitendra, and Prasanth Bodepudi. 2024. 'FACE LIVENESS DETECTION BASED ON FEATURES FUSION AND DEEP LEARNING TECHNIQUES'. *International Journal of Research in Engineering and Science* 74–80.

Devrani, Utkarsh, Sahil Saxena, and Dinesh Kumar. 2024. 'Facial Recognition-Based Automated Attendance Management System'. *International Journal of Enhanced Research in Science* 13:2319–7463.

G, Padmashree, and Karunakar A. K. 2024. 'Disguised Face Liveness Detection: An Ensemble Approach Using Deep Features'. *Cogent Engineering* 11(1). doi:10.1080/23311916.2024.2423025.

Gupta, Ashish. 2024. 'Advancements and Challenges in Face Recognition Technology'. *International Journal of Computer Trends and Technology* 72(11):92–104. doi:10.14445/22312803/IJCTT-V72I11P110.

Kamarowski, Bruno, Raul Almeida, Bernardo Biesseck, Roger Granada, Gustavo Führ, and David Menotti. 2023. *Multi-Challenge Database for Active Liveness*.

Kasture, Seema, Shruti Padale, Mansi Harihar, Aman Aatar, Sayali Ambekar, and Diploma Student. 2025. 'FACE RECOGNITION ATTENDANCE SYSTEM'. *International Research Journal of Modernization in Engineering Technology and Science* 7(3):3198–3201.

Khairnar, Smita, Shilpa Gite, Ketan Kotecha, and Sudeep D. Thepade. 2023. 'Face Liveness Detection Using Artificial Intelligence Techniques: A Systematic

Literature Review and Future Directions'. *Big Data and Cognitive Computing* 7(1). doi:10.3390/bdcc7010037.

Koshy, Ranjana, and Ausif Mahmood. 2020. 'Enhanced Deep Learning Architectures for Face Liveness Detection for Static and Video Sequences'. *Entropy* 22(10):1–27. doi:10.3390/e22101186.

Li, Lei, Zhaoqiang Xia, Jun Wu, Lei Yang, and Huijian Han. 2022. 'Face Presentation Attack Detection Based on Optical Flow and Texture Analysis'. *Journal of King Saud University - Computer and Information Sciences* 34(4):1455–67. doi:10.1016/j.jksuci.2022.02.019.

Lin, Shinfeng, D., Linares Otoya, and Paulo E. 2023. 'Pose-Invariant Face Recognition via Facial Landmark Based Ensemble Learning'. *IEEE Access*. doi:10.1109/ACCESS.2022.DOI.

Meghana, M., M. Vasavi, and D. Shravani. 2021. 'FACIAL LANDMARK DETECTION WITH MEDIAPIPE & CREATING ANIMATED SNAPCHAT FILTERS'. *International Journal for Innovative Engineering and Management Research* 11:98–107.

Nemavhola, Andisani, Colin Chibaya, and Serestina Viriri. 2025. 'A Systematic Review of CNN Architectures, Databases, Performance Metrics, and Applications in Face Recognition'. *Information (Switzerland)* 16(2). doi:10.3390/info16020107.

Ozen, Emre, Fikret Alim, Sefa B. Okcu, Enes Kavakli, and Cevahir Cigla. 2024. 'Real-Time Face Recognition System at the Edge'. P. 27 in. SPIE-Intl Soc Optical Eng.

Raj, S. Boobathi, K. Tamilselvi, and S. Mohamed Javith. 2021. 'Face Identification and Liveness Detection Using CNN for Automated Attendance System'. *International Journal of Advance Research, Ideas and Innovations in Technology* 145–48.

Ray, Debmalya. 2025. 'A Face Recognition Based Attendance System with Geolocation and Real-Time Action Logging'. *Research Square*.

Ryando, Catoer, Riyanto Sigit, and Bima Sena Bayu Dewantara. 2025. 'Face Recognition for Logging in Using Deep Learning for Liveness Detection on

Healthcare Kiosks'. *INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION* 9.

S, Pavan, and Thanuja N. 2023. 'SURVEY ON FACE RECOGNITION CNN'. *International Journal of Advanced Research in Computer and Communication Engineering ISO* 12(5):1791–95. doi:10.17148/IJARCCE.2023.125300.

Wu, Zhihao, Yushi Cheng, Jiahui Yang, Xiaoyu Ji, and Wenyuan Xu. 2023. *DepthFake: Spoofing 3D Face Authentication with a 2D Photo*. IEEE.

Zhi Jie, Ooi, Lim Tong Ming, and Tan Chi Wee. 2023. 'Biometric Authentication Based on Liveness Detection Using Face Landmarks and Deep Learning Model'. *INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION* 1057–65.